Configurar a criptografia AES nos rádios do modo IW URWB

Contents

Introdução

Este documento descreve a configuração dos parâmetros AES nos rádios IW9165 e IW9167 no modo URWB.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Navegação e comandos CLI básicos
- Compreensão dos rádios do modo IW URWB

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Rádios IW9165 e IW9167

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

AES - Advanced Encryption Standard é um padrão de criptografia para proteger a comunicação de dados. É um algoritmo de chave simétrica que significa que a mesma chave é usada para criptografar e descriptografar dados.

Os rádios IW no modo URWB usam o parâmetro de senha configurado neles para criptografar todos os dados do plano de controle.

Portanto, dois dispositivos só podem se comunicar entre si ou descobrir outros dispositivos na mesma rede se compartilharem a mesma senha.

Os dados enviados pelo plano de dados não são criptografados por padrão. Isso pode ser criptografado com a ativação do AES nos rádios.

Dois dispositivos só podem se comunicar um com o outro se ambos tiverem o AES habilitado neles.

Rotação de chaves em rádios IW:

Há outros parâmetros de segurança adicionais que podem ser configurados nos rádios IW para tornar a criptografia mais forte. Para suportar os padrões WPA, a rotação de chaves pode ser ativada nos rádios IW.

Isso é executado no protocolo controlador de chave, que permite que dois dispositivos se comuniquem entre si para agendar a regeneração periódica da nova chave transiente de par a par e da chave transiente de grupo para a criptografia de pacotes.

A PTK (Pairwise Transient Key) protege o tráfego de um para um ou unicast, enquanto a GTK (Group Transient Key) protege o tráfego de grupo ou de broadcast/multicast.

Habilitar esse recurso melhora a segurança, reduzindo a quantidade de dados que pode ser comprometida se realmente houver um ataque.

As chaves usadas para criptografia são temporárias e rodam periodicamente, portanto, não são armazenadas em nenhum lugar. Todos os outros segredos e certificados são armazenados em um volume criptografado que é protegido através do Cisco TAM.

(https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf)

Ao executar redes Fluidez, se você ativar a rotação de chaves, poderá sofrer interrupções na comunicação, especialmente se a rotação ocorrer durante o processo de roaming.

Por isso, não é recomendável ser usado junto com as implantações de fluidez.

Os parâmetros de criptografia AES podem ser configurados nos dispositivos IW somente a partir do acesso CLI ou por meio da configuração IoT OD.

Configuração CLI dos parâmetros de fluidez

Esses parâmetros podem ser configurados no modo de ativação (enable mode) no CLI dos dispositivos.

1. Configurando a senha nos rádios:

Esse parâmetro é usado para que os rádios criptografem os dados do plano de controle.

```
Radio1#configure wireless passphrase URWB
```

```
Cisco#configure wireless passphrase
  WORD  network passphrase (maximum 64 characters)
Cisco#configure wireless passphrase URWB
```

Configurar Senha Sem Fio

2. Habilitando a criptografia AES nos rádios:

Esse parâmetro permite ativar a criptografia AES por interface de rádio.

```
Radio1#configure dot11Radio

        crypto aes enable
```

```
Cisco#configure dot11Radio 1 crypto aes
  disable  disable encryption
  enable   enable encryption
Cisco#configure dot11Radio 1 crypto aes enable
```

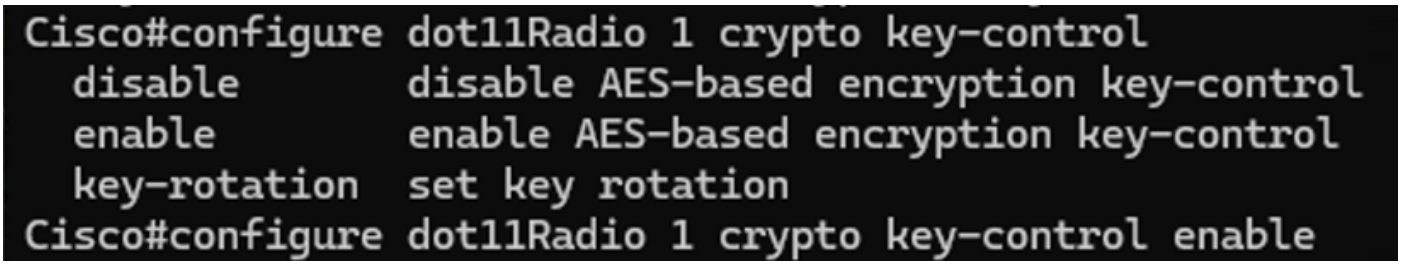
Configurar dot11Radio 1

3. Ativando o controlador principal nos rádios:

Esse parâmetro é usado para ativar o algoritmo de controlador de chave nos rádios. Isso também é habilitado por interface de rádio e é necessário para usar a rotação de chaves AES.

```
Radio1#configure dot11Radio

        crypto key-control enable
```



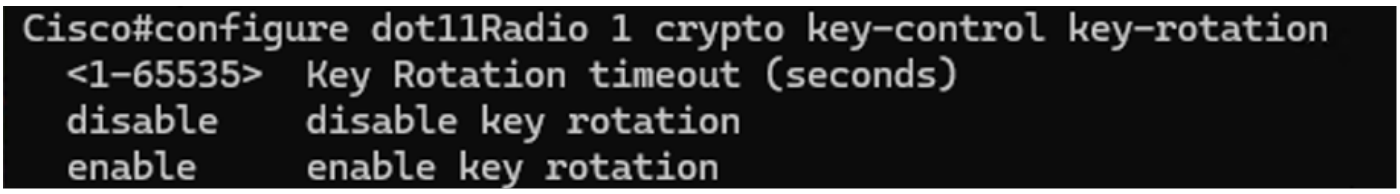
dot11Radio 1 crypto key-control

4. Ativar a rotação de chaves nos rádios:

Esse parâmetro é usado para ativar a rotação de chaves nos rádios e é ativado por interface.

Radio1#configure dot11Radio

crypto key-control key-rotation enable



Configurar dot11Radio crypto ket-rotation

5. Configure o temporizador de rotação de chaves nos rádios:

Este parâmetro é usado para configurar o intervalo de tempo no qual novas chaves são geradas. O valor do temporizador é adicionado em segundos e o parâmetro pode variar de <1-65535>.

O valor padrão é definido como 3600 segundos ou a cada hora.

Radio1#configure dot11Radio

crypto key-control key-rotation <1 – 65535>

```
Cisco#configure dot11Radio 1 crypto key-control key-rotation
  <1-65535>  Key Rotation timeout (seconds)
  disable    disable key rotation
  enable     enable key rotation
```

Configurar dot11Radio crypto ket-rotation

6. Validação dos parâmetros principais do algoritmo de controlo nos rádios:

A configuração atual no rádio com relação aos parâmetros de criptografia pode ser validada com o comando abaixo.

Radio1#show dot11Radio

crypto

```
Cisco#show dot11Radio 1 crypto

Passphrase:             d0a3c370a6b508acadf7143243890068ab602e7b1a43f1f4b9fca940b4eb6348
AES encryption:         enabled
AES key-control:        enabled
Key rotation:           enabled
Key rotation timeout:   6800(second)
Cisco#
```

Show dot11Radio 1 crypto

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.